

AGE ASSURANCE · AGE VERIFICATION · ZERO-KNOWLEDGE PROOF · BLIND SIGNATURE · HARDWARE CREDENTIAL · DIGITAL IDENTITY · COPPA · CHILD SAFETY · DISABILITY · EXCLUSION · CONTENT MODERATION · VERIFIED PEER SPACE

The Gate and the Playground

Age attestation, exclusion, and the architecture of verified peer space

How to check a child's age without identifying anyone, why every current proposal fails the children it claims to protect, and what it would take to build spaces worth verifying for.

12.5%

of minors worldwide were sexually solicited online in the past year, by the best global estimate.

The debate over protecting them has spent a decade stuck between two answers that both fail.

TWO CAMPS, ONE SHARED MISTAKE

Check everyone, or check no one

The safety camp

Verify age everywhere. Which, with today's tools, means uploading IDs and scanning faces: an identity dragnet aimed at children first.

The privacy camp

Any age check is surveillance, so build none. Which leaves a checkbox between an eight year old and everything on the internet.

Both camps assume the same thing: that checking an age means identifying a person. That assumption has been false for decades.

THE CORE CLAIM

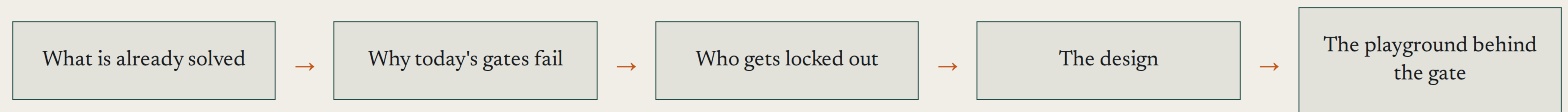
Prove one fact. Reveal nothing else. Give the proof to every child for free.

A small hardware token, issued to every child at birth the way a birth certificate is, that can answer exactly one question, over or under an age line, and that cannot be used to name, track, or profile anyone.

The hard part was never the cryptography. The hard part is who holds the credential, who pays for it, and what the verified space owes the child once she is inside.

THE ROUTE THIS DECK TAKES

Five moves



The order matters. The technology comes first so the failures can be measured against what is possible, and the playground comes last because a gate is only worth building if the space behind it is worth entering.

PART I



What Is Already Solved

The forty year old answer to the question everyone treats as new

Proving an age without revealing an identity is settled cryptography, demonstrated on real passports at real speed, and already deployed as national infrastructure in two countries.

THE PREDICATE PROOF

"Over 13" is a yes or no question. It never needed a name attached.

Cryptographers solved this in the 1980s: a credential can prove a single fact about you, over an age line, under one, while revealing nothing else, and without the checker and the issuer ever being able to compare notes.

This is running code. In 2023, researchers turned unmodified passports into anonymous age proofs that verify in under 150 milliseconds, demonstrated on exactly the age-restricted-video case legislators keep writing laws about.

SOURCES Chaum, D. (1983). Blind signatures for untraceable payments; Camenisch, J., & Lysyanskaya, A. (2001). Non-transferable anonymous credentials; Rosenberg, M., et al. (2023). zk-creds. *2023 IEEE Symposium on Security and Privacy*.

BINDING

A lost token is a paperweight

The token wakes only for its owner: a fingerprint or a PIN, checked inside the device, transmitted nowhere. Whoever finds it, steals it, or borrows it is holding an inert object.

This is the same standard your bank login already uses, and the newest credential designs go further, tying the age proof to its holder without storing a fingerprint anywhere at all. Loss is not a security problem. It is a replacement-speed problem, and replacement is part of the design: days, not weeks, through the same channel that issued the original.

NATIONAL DEPLOYMENT

Two governments already mail cryptographic identity to their residents

Estonia has issued identity documents carrying digital certificates under a statute in force since 1999. Germany's electronic identity card has operated since 2010. These are not pilots; they are decades-old civic infrastructure.

Germany also proves the paper's warning by counterexample: its card is issued on application and carries a fee set by its own regulation. A state can run flawless cryptography and still choose the two features, a form and a price, that decide who ends up outside.

The Three Failures

Why the current wave of age checks fails on its own terms

Phone-based schemes fail to bind the credential to a body, exclude the children with the least, and hand custody of childhood itself to two companies.



FAILURE ONE · BINDING

A phone proves whose phone it is. Not whose hands are on it.

Every major proposal puts the age credential in a smartphone wallet. But phones are shared objects in real households: children borrow them, unlock patterns are family knowledge, and a credential that lives in dad's phone verifies dad, wherever the phone happens to be and whoever is holding it.

A gate that cannot tell the credential holder from the credential borrower is theater with extra steps.

1 billion

people hold no official proof of identity at all. Every scheme that starts from "upload your ID" starts by excluding them.

And biometrics do not rescue the scheme: ageing, dermatological conditions, and decades of manual work each wear fingerprints past the point of recognition. Verification walls push the excluded toward less regulated corners of the internet, the exact opposite of the goal.

FAILURE TWO, CONTINUED

The data nobody collected

How often do these systems fail disabled users? Twenty-two years after biometrics became civic infrastructure, there is no current public answer. The last disability-focused government trial ran in 2004, and no serious person should quote its obsolete sensors as today's performance.

The field's own reviews admit the gap: a 2023 survey found no comprehensive accounting of elderly users' performance, a 2024 study documented both real disparities for disabled users and nondisabled people rating the systems as more inclusive than disabled users experience them, and the youth-risk literature systematically omits the children most at risk. The absence is the finding. A harm that is nobody's job to measure never appears in any evaluation of whether the system works.

FAILURE THREE · CUSTODY

Fifty bills, one destination: the phone in two companies' hands

More than fifty US state bills regulating adolescent platform access were adopted or enacted by late 2024, age verification among their most common tools, and nearly every design assumes the credential lives in a smartphone wallet. Two companies control those wallets.

Europe made the concession explicit: its 2024 digital identity regulation guarantees every citizen a free wallet credential, and its own technical work explores exactly the zero-knowledge proofs this paper describes. The cryptography is accepted. Only the custody was surrendered.

The Distributive Turn

Who gets a credential decides everything else

The paper's central move: stop asking how to verify and start asking how the proof is distributed. Issued to all at birth, free, or the gate becomes a filter on wealth and paperwork.



ENTITLEMENT, NOT APPLICATION

Issued at birth. Applied for by no one.

Where identity must be applied for, the application itself does the excluding: forms, fees, offices, and hours filter out the poorest and least connected, and the loss then cascades through every service keyed to the document. That mechanism is documented at national scale.

An applied-for credential inherits the application's failure demographics. An issued credential has none. So the token rides the one rail that already reaches nearly every child: birth registration. There is no form to fail.

WHY FREE IS NOT A DETAIL

Cost is not a line item. Cost is the filter.

The designer's instinct is to file the price under implementation, to be sorted out at appropriations. That instinct is the error this paper exists to name: a fee selects who is inside the system and who is out, with a precision no written eligibility rule could match.

And what the priced-out child loses is not one act on one day. It is ordinary participation in the medium where education, healthcare information, community, and friendship now live. Germany already shows a mature state choosing a fee on top of working cryptography. This design refuses that choice in the statute itself.

THE AUTHOR'S OWN DESIGN, AUDITED

The proposal takes its own test

The paper turns its harm analysis on itself and reports what survives. At-birth issuance removes application failure, but it cannot remove biometric enrollment failure, and the honest finding is that nobody knows that failure's true size, because the disability-disaggregated data was last collected in 2004.

And an infant cannot enroll a fingerprint at all: newborn ridges change as the hand grows. So the youngest band runs on guardian-held delegation, which is exactly the abuse surface the paper's own limits section names as unsolved. The architecture cannot bind a person who does not yet have a stable body, and the paper says so instead of hiding it.

IV

Two Credentials and a Ceremony

What the token says, what the guardian signs, and why the signup happens in person

An attestation that speaks one fact, a delegation that records a guardian's revocable yes, and a signup ceremony built so that nobody, issuer included, can follow the child afterward.

TWO DIFFERENT STATEMENTS

The token can say two things, and only two

1

■ Attestation

Over the line, or under it. Nothing else: no name, no birthday, no record of where it was asked. The platform learns one bit and cannot connect this visit to any other.

2

■ Delegation

A guardian's recorded, specific, revocable yes: this child may enter this space, on these terms. Today's checkbox regime cannot record that yes at all, so the engaged parent's only option is to help the child lie, and research confirms parents do exactly that, routinely, by creating the accounts themselves.

WHAT DELEGATION RETURNS

The most researched decision in the house

A fourteen year old with autism, ADHD, and an intellectual disability wants to write fan fiction with a conversational AI: structured, low-stakes practice at exactly the social exchange that is hardest for him. His parent studies it, sets terms with him, and says yes.

The evidence says that yes matters most for exactly this child: adolescents with special educational needs face elevated online risk, active parental engagement reduces it for them in particular, and the practice itself shows measurable gains. Today's terms of service make that parent's researched yes indistinguishable from neglect. Delegation makes it legible, specific, and revocable.

PHYSICAL PRESENCE, THEN SILENCE

Signed up in person. Followed by no one.

Enrollment happens in person, the way passports do, because presence is the one thing a remote attacker cannot fake. Where a space involves recording between members, consent runs both ways: both tokens agree, or the feature stays off.

Then the crucial property: unlinkability. The issuer learns a mailing address and nothing after. Two presentations of the same token cannot be matched to each other, so no one, issuer, platform, or eavesdropper, can assemble the child's trail. This is not a policy promise to behave. It is math about what the records can contain.

PART V

The Verified Playground

What the gate is for

Verification buys composition: a space where everyone is who the band says. What happens inside, supervision, consent, and memory, is what the whole gate was for.



COMPOSITION, THEN SUPERVISION

The gate sets who is inside. It cannot govern what happens there.

Here is the finding that breaks every gate-only proposal: the best national data shows minors are harmed online mostly by dating partners, friends, and acquaintances, not by adult strangers. A perfect gate that excludes every unverified adult still leaves most of the threat model standing, inside, among verified peers.

So the design pairs the gate with a supervision layer that is the point rather than the afterthought: trained human moderation, made legitimate by the delegation every guardian signed. The gate establishes the population. The supervision catches what the gate never could.

THE HONEYPOT OBJECTION, ANSWERED WITH ARITHMETIC

"You built a target." Fine. Then measure it.

Concentrating verified children in one place creates an attractive target; the objection is fair and the paper does not wave it away. It converts it into an operating condition that can be monitored: the space earns its existence only while the rate of harm inside, compromises times detection failures, stays below the open internet's ambient rate.

And that ambient rate is not hypothetical. It is 12.5 percent of minors solicited per year. The bar the verified space must beat is published, global, and grim.

THE CAMERA IN THE CORNER

Delete everything, and you delete the evidence she was not ready to ask for

Children delay disclosing abuse. Not occasionally: in a national sample of 8,503 people, 45 percent of survivors had never told anyone, and those who did waited a mean of 7.1 years. When a child finally speaks, the first listener is usually a peer, plausibly inside the very space where it happened.

A zero-retention rule destroys the record years before she is ready. So the design keeps supervised-space records sealed in escrow: never advertising material, never training data, never browsable, openable only by legal process when she speaks. Memory, held for her, used by no one else.



The Discharge and the Limits

What verification must never buy, and what this design still cannot do

Compliance has a documented habit of becoming a symbol that courts eventually bless. The rule against it must live in the architecture, and the design must state its own failures out loud.

THE DISCHARGE FAILURE

"We verified" must never finish the sentence "so it is not our fault"

The sociology of law has documented this pattern for decades: give organizations a legal requirement and they build visible symbols of compliance, shaped as much by managerial interest as by the goal. Then the second act makes it worse: courts come to defer to the symbols, granting legal benefit to the gesture itself.

Applied here: hand platforms a verification mandate and verification becomes the liability shield, while the duty of care inside the space evaporates. That is why this design writes the no-discharge rule into the architecture instead of trusting enforcement discretion, because the record shows discretion is exactly where the pattern completes.

SIX LIMITS, STATED PLAINLY

1 The guardian who is the threat

An adult with physical control can force any unlock. No token fixes that; reporting, supervision, and criminal law exist for exactly this.

3 The unwritten invoice

No honest price exists; the last comparable trial ran in 2004. Birth certificates and Social Security numbers were once new line items a government simply chose to fund.

5 The bystander

A gate checks whoever approaches it. The child walking past an ambient camera approaches nothing; protecting her takes a law aimed at the device, not the doorway.

2 The lost token is a paperweight

A finder or thief gets nothing. The real cost is the wait, so replacement ships in days through the issuing channel, and worn-out cryptography swaps keys without reissuing tokens.

4 The band boundary

Children grow continuously; bands move in steps. Friends made inside a space get split when one crosses a line, and the paper has no clean fix.

6 Adoption

Only a government can do this, and the firms best placed to build the wallet alternative profit if wallets win. Waiting for industry means waiting forever.

THE CLAIM, RESTATED

The gate was never the hard part

The cryptography is forty years old. Two governments already run the mail. What has been missing is a pair of decisions: to hand the proof to the child instead of the platform, free and at birth, and to admit that a gate is only worth building when the space behind it, supervised, consent-bound, and honest about its memory, is worth a childhood spent inside it.

Check the age. Tell no one who she is. And build the playground, because that was the point of the fence all along.

Gilly, T. (2026). *The Gate and the Playground: Age Attestation, Exclusion, and the Architecture of Verified Peer Space*. Working paper, July 2026.

Alaggia, R., Collin-Vézina, D., & Lateef, R. (2017). Facilitators and barriers to child sexual abuse (CSA) disclosures: A research update (2000–2016). *Trauma, Violence, & Abuse*, 20(2), 260–283.

Bundesrat Drucksache 139/21, *Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät* [Draft Act introducing electronic proof of identity on a mobile device] (Ger. Feb. 12, 2021). <https://dip.bundestag.de/drucksache/139-21/250501>

Cabello-Hutt, T., Cabello, P., & Claro, M. (2018). Online opportunities and risks for children and adolescents: The role of digital skills, age, gender and parental mediation in Brazil. *New Media & Society*, 20(7), 2411–2431.

Camenisch, J., & Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In B. Pfitzmann (Ed.), *Advances in Cryptology: EUROCRYPT 2001* (pp. 93–118). Springer.

Carah, N., Demaio, S., Holly, L., Kickbusch, I., & Williams, C. (2024). Beyond banning: Our digital world must be made safer for young people. *Health Promotion Journal of Australia*, 36(1). <https://doi.org/10.1002/hpja.938>

Cavallini, C., et al. (2025). Early adolescents and exposure to risks online: What is the role of parental mediation styles? *Social Sciences*.

Chaudhuri, B. (2022). Programmed welfare: An ethnographic account of algorithmic practices in the public distribution system in India. *New Media & Society*, 24(4), 887–902. <https://doi.org/10.1177/14614448221079034>

Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), *Advances in Cryptology: Proceedings of Crypto 82* (pp. 199–203). Springer.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

Chudnovsky, M., & Peeters, R. (2021). A cascade of exclusion: Administrative burdens and access to citizenship in the case of Argentina's national identity document. *International Review of Administrative Sciences*.

Collings, S. J., Griffiths, S., & Kumalo, M. (2005). Patterns of disclosure in child sexual abuse. *South African Journal of Psychology*, 35(2), 270–285. <https://doi.org/10.1177/008124630503500207>

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3, 1376. <https://doi.org/10.1038/srep01376>

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, 347(6221), 536–539. <https://doi.org/10.1126/science.1256297>

- Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis* [eID-Karte-Gesetz] [Act on a card for Union citizens and EEA nationals with an electronic proof of identity function] (Ger. June 21, 2019). <https://www.gesetze-im-internet.de/eidkg/>
- Common Sense Media. (2025, April 10). *AI risk assessment: Social AI companions*. Common Sense Media. (Rating: unacceptable; use case review; conducted with input from the Stanford Brainstorm Lab for Mental Health Innovation.)
- Edelman, L. B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American Journal of Sociology*, 97(6), 1531–1576.
- Edelman, L. B., Uggen, C., & Erlanger, H. S. (1999). The endogeneity of legal regulation: Grievance procedures as rational myth. *American Journal of Sociology*, 105(2), 406–454.
- European Parliament and Council. (2024). Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*, L, 2024/1183.
- Fairhurst, M., Li, C., & Da Costa-Abreu, M. (2017). Predictive biometrics: A review and analysis of predicting personal characteristics from biometric data. *IET Biometrics*, 6(6), 369–378. <https://doi.org/10.1049/iet-bmt.2016.0169>
- Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. *JAMA Network Open*, 5(10), e2234471.
- Fry, D., et al. (2025). Prevalence estimates and nature of online child sexual exploitation and abuse: A systematic review and meta-analysis. *The Lancet Child & Adolescent Health*.
- Gambs, S., Killijian, M.-O., & Núñez-del-Prado Cortez, M. (2014). De-anonymization attack on geolocated data. *Journal of Computer and System Sciences*, 80(8), 1597–1614. <https://doi.org/10.1016/j.jcss.2014.04.024>
- Gilly, T., & Mattheus, R. (2026). Harm blindness in digital child protection policy: A systematic stakeholder, sentinel and legal analysis of Australia's under-16 social media ban. In K. Ringmar Sylwander, G. Shekhawat, & S. Livingstone (Eds.), *Children's rights under pressure in a digital world: Proceedings of the International Communication Association pre-conference* (pp. 60–65). Digital Futures for Children centre, LSE and 5Rights Foundation. <https://researchonline.lse.ac.uk/id/eprint/138632/>
- Isikut tõendavate dokumentide seadus* [Identity Documents Act] (Est. Feb. 15, 1999), Riigi Teataja. <https://www.riigiteataja.ee/akt/77253>
- Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, 67(1), 82–105.
- Martin, A., et al. (2020). Exclusion and inclusion in identification: Regulation, displacement and data justice. *Information Technology for Development*.

- Manay, N., & Collin-Vézina, D. (2019). Recipients of children's and adolescents' disclosures of childhood sexual abuse: A systematic review. *Child Abuse & Neglect*, 98, 104192.
- Mathews, B., et al. (2025). Characteristics of first disclosure of child sexual abuse: Age, delay, recipient, and feeling of support. *Child Abuse & Neglect*.
- McElvaney, R. (2013). Disclosure of child sexual abuse: Delays, non-disclosure and partial disclosure. What the research tells us and implications for practice. *Child Abuse Review*, 24(3), 159–169. <https://doi.org/10.1002/car.2280>
- Mukherjee, A., & Sahay, S. (2019). Sinking under its own weight: Case of Aadhaar mediated entitlements in India. In P. Nielsen & H. C. Kimaro (Eds.), *Information and Communication Technologies for Development: Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D* (pp. 472–485). Springer. https://doi.org/10.1007/978-3-030-18400-1_39
- Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE. <https://doi.org/10.1109/SP.2008.33>
- Personalausweisgesetz* [PAuswG] [Identity Card Act] (Ger. June 18, 2009), BGBl. I at 1346.
- Personalausweisgebührenverordnung* [PAuswGebV] [Regulation on fees for identity cards and eID cards for Union citizens and EEA nationals] (Ger. Nov. 1, 2010). <https://www.gesetze-im-internet.de/pauswgebv/>
- Personalausweisverordnung* [PAuswV] [Regulation on identity cards, eID cards for Union citizens and EEA nationals, and electronic proof of identity] (Ger. Nov. 1, 2010). <https://www.gesetze-im-internet.de/pauswv/>
- Ólafsdóttir, B., et al. (2024). A case study on the inclusiveness of biometric technologies for individuals with congenital disabilities. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*. ACM.
- Poh, N., et al. (2025). Biometric bound credentials for age verification. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*.
- Rao, U., & Nair, V. (2019). Aadhaar: Governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469–481. <https://doi.org/10.1080/00856401.2019.1595343>
- Riaz, I., et al. (2024). Loss of fingerprint features and recognition failure due to physiological factors: A literature survey. *Multimedia Tools and Applications*.
- Rose, S. E., & Middling, L. R. (2025). Preteens social media use: Parents' and children's perceptions of what mediation approaches are used and why. *British Journal of Developmental Psychology*, 43(3), 771–786. <https://doi.org/10.1111/bjdp.12552>

- Rosenberg, M., White, J., Garman, C., & Miers, I. (2023). zk-creds: Flexible anonymous credentials from zkSNARKs and existing identity infrastructure. In *2023 IEEE Symposium on Security and Privacy* (pp. 790–808). IEEE.
- Samdal, O., Budin-Ljøsne, I., Haug, E., Helland, T., et al. (2023). Encouraging greater empowerment for adolescents in consent procedures in social science research and policy projects. *Obesity Reviews*, 24(S2). <https://doi.org/10.1111/obr.13636>
- Schittenhelm, C., et al. (2024). Cybergrooming victimization among young people: A systematic review of prevalence rates, risk factors, and outcomes. *Adolescent Research Review*.
- Thimm-Kaiser, M., & Keyes, K. M. (2025). US state policies regarding social media: Do policies match the evidence? *The Milbank Quarterly*, 103(S1), 337–365. <https://doi.org/10.1111/1468-0009.70021>
- Wang, K., et al. (2023). Biometrics-based mobile user authentication for the elderly: Accessibility, performance, and method design. *International Journal of Human-Computer Interaction*.
- UK Passport Service. (2005). *Biometrics enrolment trial: Report*. Atos Origin.
- UKPS biometric enrolment trial*. (2005). Biometric Technology Today. <https://www.sciencedirect.com/science/article/abs/pii/S0969476505703684>
- W3C. (2021). *Web Authentication: An API for publicly accessing public key credentials, Level 2* [W3C Recommendation]. World Wide Web Consortium. <https://www.w3.org/TR/webauthn-2/>
- Zafeiropoulou, A., et al. (2025). Age verification in the context of the EUDI Wallet: Balancing privacy and security. In *Proceedings of the 16th International Conference on Information, Intelligence, Systems and Applications (IISA)*. IEEE.
- Zhong, W., Luo, J., Luo, L., & Lyu, Y. (2025). The role of social robot in enhancing social–emotional skill development in children with autism: A three-level meta-analysis. *Journal of Computer Assisted Learning*, 41(6). <https://doi.org/10.1111/jcal.70154>